WHAT IS CLAIMED IS:

1. A PKI certificate architecture for a network connected gaming system, wherein each software component within the gaming system subject to receive certification is signed with a distinctive certificate, the certificate being uniquely identified by at least one field.

2. A PKI certificate architecture according to claim 1, wherein the each software component is authorized by a regulatory authority.

3. A PKI certificate architecture according to claim 1, wherein the distinctive certificate is produced by the certification lab, by the gaming system supplier or by the trusted party designated by the regulatory authority.

4. A PKI certificate architecture according to claim 1, wherein each software component is signed by the certification lab, by the gaming system supplier or by the trusted party designated by the regulatory authority.

5. A PKI certificate architecture according to claim 1, wherein the at least one field is the field denoted as the "issued to" field, the "subject name" field, the "CommonName" field or the "publisher" field.

6. A PKI certificate architecture according to claim 1, wherein the at least one field comprises at least one of fields and field extensions.

7. A PKI certificate architecture according to claim 1, wherein the at least one field comprises at least one of:

a software component part number;

a software component major version number;

a software component minor version number;

a software component build number;

a software component revision number;

a software component project name;

a software component type of software component;

a software component language variant;

a software component game regulation variant;

a software component friendly name;

an identification of the certification laboratory, and

an identification of the client.

8. A PKI certificate architecture according to claim 7, wherein each of the at least one field is a concatenation of a selected set of fields.

9. A PKI certificate architecture according to claim 1, wherein at least a portion of the at least one field is reported in the windows event log upon execution of the software component.

10. A PKI certificate architecture according to claim 1, wherein at least a portion of the at least one field is reported in the source field of the windows event log upon execution of the software component.

11. A PKI certificate architecture according to claim 1, wherein at least a portion of the at least one field is reported in the windows event log upon execution of the software component in a predetermined event log bin upon execution of the software component.

12. A PKI certificate architecture according to claim 1, wherein at least a portion of the at least one field is traceable in at least one of:

source code;

Windows File Properties;

Trusted Inventory;

Windows Event Log;

Software Restriction Policies, and

Certificate Store.

13. A PKI certificate architecture according to claim 1, wherein the network connected gaming system is connected in at least one of a local area system and wide area network.

14. A PKI certificate architecture according to claim 1, wherein the network connected gaming system comprises gaming terminals and/or gaming servers.

15. A PKI certificate architecture according to claim 1, wherein the at least one field contains identification information delimited with file-name-allowed non-alphanumeric characters to facilitate human identification, string searches and file searches.

16. A PKI certificate architecture according to claim 1, wherein a selected set of identification information making up the at least one field are used for making up the file name of PKI certificate related files such as *.CER, *.P7B and *.PVK such as to facilitate human identification, string searches and file searches.

17. A method for a network connected gaming system to prevent unauthorized software components from executing, comprising the steps of:

producing a separate PKI certificate for each software component subject to receiving certification;

code signing each software component subject to receiving certification with its respective PKI certificate, and

configuring Software Restriction Policy certificate rules to allow execution of a selected set of each software component subject to receiving certification.

18. A method according to claim 17, further comprising the step of configuring Software Restriction Policy rules to prevent execution of unauthorized software.

19. A method according to claim 17, further comprising the step of configuring Software Restriction Policy rules to prevent execution of all not explicitly authorized software.

20. A method for a network connected gaming system to enable only authorized software components to execute, comprising the steps of:

configuring a Software Restriction Policy for each authorized software component, and

enforcing the Software Restriction Policy.

21. A method for a network connected gaming system according to claim 20, wherein the authorized software components are mandated by a regulatory body.

22. A method for a network connected gaming system to enable only authorized software components to execute, comprising the steps of:

configuring a certificate Software Restriction Policy for each authorized software component;

configuring a path Software Restriction Policy to prevent unauthorized software components from executing;

configuring a path Software Restriction Policy to prevent non-explicitly authorized software components from executing;

enforcing the certificate Software Restriction Policies, and

enforcing the path Software Restriction Policies.

23. A method for a network connected gaming system according to claim 22, wherein the authorized software components are mandated by a regulatory body.

24. A method for a network connected gaming system to enable only authorized software components to execute, comprising the steps of:

producing a separate PKI certificate for each software component subject to receive certification;

signing each software component subject to receive certification with the its respective separate PKI certificate;

configuring a certificate Software Restriction Policy for each of the respective separate PKI certificates, and

enforcing the certificate Software Restriction Policy for each of the respective separate PKI certificates.

25. A method for downloading authorized software components for a network connected gaming system, comprising the steps of:

code signing each authorized software component with a distinctive PKI certificate;

configuring install policies to install each code signed authorized software component;

configuring certificate rule policies to allow execution of the installed code signed authorized software component;

configuring enforcement of the policies.

26. A method for a network connected gaming system to enable selective execution of at least one authorized software component, comprising the steps of:

configuring Software Restriction Policies for the at least one authorized software component at a predetermined time;

unrestricting the Software Restriction Policies for the at least one authorized software component at a predetermined time;

enabling a link for the Software Restriction Policies for the at least one authorized software component at a predetermined time;

checking for a change of the Software Restriction Policies and if there is no policy change then looping to the beginning of this step, and

enforcing the change of the Software Restriction Policies at a predetermined time.

27. A method for a network connected gaming system according to claim 26, wherein the checking step includes checking for the change of the Software Restriction Policies whenever a predetermined timeout has expired subsequent to the player balance reaching zero and if there is no policy change then looping to the beginning of this step.

28. A method for a network connected gaming system according to claim 26, further comprising the step of displaying a list of authorized software to the player for selection.

29. A method for a network connected gaming system according to claim 26, wherein a rule for the Software Restriction Policies is at least one of certificate rule, path rule, hash rule, Internet zone rule and registry path rule.

30. A method for a network connected gaming system according to claim 26, wherein the network connected gaming system is connected in at least one of a local area system and a wide area network.

31. A method for a network connected gaming system according to claim 26, wherein the network connected gaming system comprises at least one of gaming terminals and gaming servers.

32. A method for a network connected gaming system according to claim 26, wherein the checking step includes executing the RegisterGPNotification function.

33. A method for a network connected gaming system according to claim 26, wherein the checking step is bypassed.

34. A method for a network connected gaming system according to claim 26, wherein the enforcing step includes executing the gpupdate function.

35. A method for a network connected gaming system according to claim 26, wherein the enforcing step includes executing the gpupdate function followed by a reboot.

36. A method for a network connected gaming system according to claim 26, wherein the enforcing step includes executing the RefreshPolicy or RefreshPolicyEx function.

37. A method for a network connected gaming system according to claim 26, wherein the enforcing step includes executing the RefreshPolicy or RefreshPolicyEx function followed by a reboot.

38. A method for a network connected gaming system according to claim 26, further comprising the steps of:

configuring Software Installation Policies for the at least one authorized software component at a predetermined time;

enabling a link for the software installation policies for the at least one authorized software component at a predetermined time;

checking for a change of the Software Installation Policies and if there is no policy change then looping to the beginning of this step, and

enforcing the change of the software installation policies.

39. A method for a network connected gaming system according to claim 38, wherein the checking step includes checking for the change of the software installation policies whenever a predetermined timeout has expired subsequent to the player balance reaching zero and if there is no policy change then looping to the beginning of this step.

40. A method for a network connected gaming system according to claim 38, wherein the checking step includes executing the RegisterGPNotification function.

41. A method for a network connected gaming system according to claim 38, wherein the checking step is bypassed.

42. A method for a network connected gaming system according to claim 38, wherein the enforcing step includes executing the gpupdate function.

43. A method for a network connected gaming system according to claim 38, wherein the enforcing step includes executing the gpupdate function followed by a reboot.

44. A method for a network connected gaming system according to claim 38, wherein the enforcing step includes executing the RefreshPolicy or RefreshPolicyEx function.

45. A method for a network connected gaming system according to claim 38, wherein the enforcing step includes executing the RefreshPolicy or RefreshPolicyEx function followed by a reboot.

46. A method for a network connected gaming system according to claim 38, further comprising the step of displaying a list of authorized software to the player for selection.

47. A method for a network connected gaming system according to claim 26, further comprising the initial steps of:

monitoring the game activity of players, and

choosing the at least one authorized software components in order to adapt game offering on the gaming terminals.

48. A method for a network connected gaming system according to claim 47, wherein the monitoring and choosing steps are carried out in a close-loop fashion such as to optimize player game activity in real-time.

49. A method for a network connected gaming system to enable selective availability of games on gaming terminals, comprising the steps of:

installing a plurality of game software on a selected set of gaming terminals;

choosing a selected set of installed game software to offer to players of the gaming terminals;

a first activating the chosen selected set of installed game software on a selected set of gaming terminals;

monitoring the game activity of the players on a selected set of gaming terminals;

modifying the selected set of installed game software to offer to players;

a second activating the modified selected set of installed game software on a selected set of gaming terminals;

50. A method for a network connected gaming system according to claim 49, wherein the monitoring, modifying and activating steps are executed in a close-loop fashion such as to optimize player game activity in real-time.

51. A method for a network connected gaming system according to claim 49, further comprising the step of displaying a list of authorized software to the player for selection.

52. A method for a network connected gaming system according to claim 49, further comprising a step of downloading at least one authorized game software to a selected set of the of gaming terminals;

53. A method for a network connected gaming system to enable selective availability of games on PC based gaming terminals, comprising the steps of:

selecting game software to be made available to players on a selected set of gaming terminals;

terminating all gaming software on a selected set of gaming terminals to transform each gaming terminals into a generic PC communicating in the network connected gaming system;

downloading via the network the selected game software to the generic PCs, and

starting the game software to transform the generic PCs into gaming terminals.

54. A method for a network connected gaming system according to claim 53, further comprising the step of displaying an “out-of-service” message or equivalent message to the player while the gaming terminal is transformed into a generic PC.

55. A method for a network connected gaming system according to claim 53, further comprising the step of displaying a list of software to the player for selection.

56. A method for a network connected gaming system according to claim 53, wherein the game software is authorized by a regulatory authority.

57. A method for a network connected gaming system according to claim 53, wherein booting is at least one of cold-booting, hot-booting and power-on booting.

58. A method for a network connected gaming system according to claim 53, wherein the PC based gaming terminals run a version of the Microsoft Windows operating system

59. A method for a network connected gaming system according to claim 53, wherein the step of downloading game software uses the Software Installation Policy (SIP) feature of the Windows operating system.

60. A method for a network connected gaming system according to claim 53, wherein the step of downloading game software uses the Microsoft SMS Systems Management Server.

61. A method for a network connected gaming system according to claim 53, further comprising the step of preventing unauthorized software from executing using the Software Restriction Policy feature.

62. A method for a network connected gaming system to enable selective availability of games on PC based gaming terminals, comprising the steps of:

selecting game software to be made available to players on a selected set of gaming terminals;

terminating all gaming software on a selected set of gaming terminals to transform each gaming terminal into a generic PC communicating in the network connected gaming system;

booting the generic PCs;

starting an operating system on the generic PCs;

downloading via the network the selected game software to the generic PCs, and

starting the game software to transform the generic PCs into gaming terminals.

63. A method for a network connected gaming system according to claim 62, further comprising the step of displaying an "out-of-service" message or equivalent message to the player while the gaming terminal is transformed into a generic PC.

64. A method for a network connected gaming system according to claim 62, further comprising the step of displaying a list of software to the player for selection.

65. A method for a network connected gaming system according to claim 62, wherein the game software is authorized by a regulatory authority.

66. A method for a network connected gaming system according to claim 62, wherein booting is at least one of cold-booting, hot-booting and power-on booting.

67. A method for a network connected gaming system according to claim 62, wherein PC based gaming terminals run a version of the Microsoft Windows operating system.

68. A method for a network connected gaming system according to claim 62, wherein the step of downloading game software uses the Software Installation Policy feature of the Windows operating system.

69. A method for a network connected gaming system according to claim 62, further comprising the step of preventing unauthorized software from executing using the Software Restriction Policy feature.

70. A method for a network connected gaming system according to claim 62, wherein the step of downloading game software uses the Microsoft SMS Systems Management Server.

71. A method for a network connected gaming system to prevent unauthorized executable files from executing, comprising the steps of:

packaging the authorized executable files into a code signed MSI installation package;

configuring certificate rule policies to enable execution of the code signed MSI installation package;

enforcing the policies, and

executing the code signed MSI installation package upon every computer startup or upon a command.

72. A method for a network connected gaming system according to claim 71, wherein the code signing uses a distinctive PKI certificate for each MSI installation package.

73. A method for a network connected gaming system to prevent unauthorized executable code from executing, comprising the steps of:

packaging the authorized executable files into a code signed MSI installation package;

configuring certificate rule policies to enable execution of the code signed MSI installation package;

configuring enforcement of the policies, and

re-installing the code signed MSI installation package at every computer startup or upon a command.

74. A method for a network connected gaming system according to claim 73, wherein the code signing uses a distinctive PKI certificate for each MSI installation package.

75. A method for a network connected gaming system to prevent unauthorized non-executable files to affect game outcome, comprising the steps of:

packaging the non-executable files into a code signed MSI installation package;

configuring certificate rule policies to enable execution of the code signed MSI installation package;

configuring enforcement of the policies, and executing the code signed MSI installation package upon every computer startup or upon a command.

76. A method for a network connected gaming system according to claim 75, wherein the code signing uses a distinctive PKI certificate for each MSI installation package.

77. A method for trusting at least one authorized non-executable software component certified to comply with regulatory requirements downloaded into a network connected gaming system, comprising the steps of:

packaging the at least one non-executable file into at least one code signed MSI installation package;

configuring certificate rule policies to enable execution of the at least one code signed MSI installation package;

configuring enforcement of the policies, and

re-installing the at least one code signed MSI installation package at every computer startup or upon a command.

78. A method for a network connected gaming system according to claim 77, wherein the at least one code signing uses a distinctive PKI certificate for each of the at least one MSI installation package.

79. A method for scheduling at least one authorized executable software component installed in a network connected gaming system, comprising the steps of:

packaging at least one authorized non-executable file that control the scheduling of the at least one authorized executable software component into at least one code signed MSI installation package;

configuring certificate rule policies to enable execution of the at least one code signed MSI installation package in a selected set of gaming terminals; and

configuring enforcement of the certificate rule policies; and

downloading the at least one code signed MSI installation package into a selected set of gaming terminals;

executing the at least one code signed MSI installation packages.

80. A method for scheduling at least one authorized executable software component according to claim 79, wherein the code signing uses a distinctive PKI certificate for each of the at least one MSI installation package.

81. A method for scheduling at least one authorized executable software component according to claim 79, further comprising the step of re-installing the at least one code signed MSI installation package at every computer startup or upon a command.

82. An automated platform to enable the on-going regulatory certification of a substantial number of authorized software components, comprising:

a reference platform representative of a target network connected gaming system and comprising a software-building environment located at the manufacturer's premises or designated subcontractors;

a certification platform located at a regulatory certification authority substantially identical to the reference platform, and

code-signing means for associating a distinctive PKI certificate with each authorized software component.

83. An automated platform according to claim 82, further comprising a secure communication link for enabling manufacturer or designated subcontractors to remotely configure the software build environment on the certification platform.

84. An automated platform according to claim 82, wherein the target code to be downloaded to the network connected gaming system is tested by the certification laboratory.

85. An automated platform according to claim 82, wherein the target code to be downloaded to the network connected gaming system is compiled by the certification laboratory.

86. An automated platform according to claim 82, further comprising a secure communication link for enabling remote assistance.

87. An automated platform according to claim 82, further comprising a secure communication link for enabling users to carry out certification steps from a remotely located computer.

88. An automated platform according to claim 82, wherein the code signing means comprises a certificate authority under control of the manufacturer for generating certificates.

89. An automated platform according to claim 82, wherein the code signing means comprises a certificate authority under control of the regulatory certification authority for generating certificates.

90. An automated platform according to claim 82, wherein the software-building environment of the reference platform and the software-building environment of the certification platform are maintained synchronized.

91. A method for a gaming terminal in a network connected gaming system to generate a list of authorized games available to the players comprising the steps of:

enforcing Software Restriction Policy for preventing non-authorized software components from executing;

enforcing Software Restriction Policy for enabling execution of a selected set of authorized games;

attempting to execute each game, and

adding games that have not been denied execution to a menu list.

92. A method for a network connected gaming system according to claim 91, further comprising the step of removing games from the menu list for games that have been denied execution.

93. A method for a network connected gaming system according to claim 91, further comprising the step of removing games from the menu list for games whose executable file are not found .

94. A method for a gaming terminal in a network connected gaming system to generate a list of authorized games available to players comprising the steps of:

generating an executable companion file for each authorized game, wherein the executable companion file is substantially quicker to execute than starting execution of the game and, wherein the code-signed PKI certificate associated to the companion file is identical to the code-signed PKI certificate associated to the game main module;

enforcing Software Restriction Policy for preventing non-authorized software components from executing;

enforcing Software Restriction Policy for enabling execution of a selected set of authorized games;

attempting to execute each companion file, and adding only those games to a menu list whose companion file has not been denied execution.

95. A method for a network connected gaming system according to claim 94 further comprising the step of removing games from the menu list for games whose companion file is denied execution.

96. A method for a network connected gaming system according to claim 94, further comprising the step of removing games from the menu list for games whose companion executable file is not found.